SAS 70 Certification:

A New Imperative for Meeting Customer Needs

Crowe®

The Unique Alternative to the Big Four®

Growing regulatory requirements are making corporate customers more aware of their vendors' internal controls and security than ever before. Maintaining an up-to-date SAS 70 report based on an audit of the effectiveness of a company's control objectives and activities can go a long way toward satisfying these customers' concerns. To successfully navigate the SAS 70 audit process, it is important to know as much as possible about what auditors are looking for and how to support a successful audit process.

In this age of greater regulation, simply meeting customer needs with superior products and services may no longer be enough. Indeed, getting and retaining the business of corporations that must comply with the *Sarbanes-Oxley Act of 2002* (SOX), the *Health Insurance Portability and Accountability Act* (HIPAA), and other regulations could mean being prepared to disclose comprehensive information about internal operations, particularly security and other internal controls.

SOX Section 404 requires public companies to document and test their internal controls and then have an external auditor issue an opinion on management's design and operating effectiveness of those controls. This may include controls related to vendor management functions. As a result, these companies are working to understand what services their vendors provide on their behalf and the controls those vendors have in place surrounding these services.

SOX Section 404 has been in effect for the largest market-capital public companies since 2004. The law has been fully phased in this year so all public companies, regardless of size, must comply with the law. External auditor opinions on design and effectiveness of controls will not be required until 2008.

HIPAA requires, among other things, the safeguarding of private health-related information and affects companies in the healthcare and insurance industries, as well as employer-provided health plans. Many companies that maintain protected health information rely on vendors for their information technology (IT) systems and are beginning to ask these vendors about the specific controls and protection surrounding that information.

If vendors have not yet been asked for control-related information from publicly traded corporate customers, or even customers who, in turn, are vendors of those companies, they soon will be facing a similar inquiry. However, simply having proof that a vendor has internal controls will not be enough for these customers.

Instead, vendors are likely to be fielding new requests for information not only on the existence of internal controls but also on their effectiveness. Much of the focus will be on internal controls for the vendor's information technology and processes in general and the technology and processes involving customer information and data specifically.

To obtain this information, many customers will simply ask for something called a SAS 70 report. And if the vendor is unable to produce that report, it could find even its strongest customer relationships compromised. In some cases, vendors without a SAS 70 report have had multiple customers sending their own internal auditors to assess the vendor's internal controls. Even though clients' internal auditors ask for the same information, the frequency of these requests and the resulting disruption can prevent many individuals in these vendor organizations from completing their normal work. As a result, many vendors have obtained a SAS 70 report to avoid these client intrusions.

The SAS 70 Report

An audit based on Statement on Auditing Standards No. 70 (SAS 70), "Reports on the Processing of Transactions by Service Organizations," gauges the effectiveness of a company's control objectives and activities throughout its operations, particularly those related to technology, customer data, and security.

SAS 70 was developed by the American Institute of Certified Public Accountants and rolled out in March 1993. Since then, the SAS 70 report has become the standard attestation and communication vehicle covering control design and operating effectiveness in the United States and is currently the most common vehicle for relaying control-related information. It is important to note that, even though SAS 70 is a U.S. standard, non-U.S. companies can undergo an audit to obtain a SAS 70 report if they provide services to U.S. companies.

The audit and its related report allow a company to show its customers that it has appropriate controls and safeguards to handle data and information belonging to the customer. Being able to produce this information on demand, certified by an objective third party, and in a recognized and standardized format, is extremely important to customers in this regulatory environment.

There are many other benefits associated with having a SAS 70 report. For example, when a company satisfies SAS 70 requirements, it has introduced certain checks and balances into the operating environment that can minimize disruptions and increase overall efficiency.

Two Types of Reports

There are two types of SAS 70 reports. A Type I report covers the design effectiveness of controls as of the date of the report. A Type II report covers the design of the controls and the operating effectiveness of the controls over a period of time specified in the opinion and tested by the auditor. A Type II report provides detailed information and testing that shows where the control objectives achieved operating effectiveness and the only one that generally meets the requirements of SOX Section 404.

While a Type II report provides more complete coverage regarding the operating effectiveness over a period of time, a company often opts for a Type I report if 1) the company needs a report quickly, 2) the company has included relatively new operations or systems with limited history for testing, or 3) the company is completing its first SAS 70 certification. Yet, even in these cases, the Type I report would typically be followed by a Type II report within six months to a year.

Regardless of the type of report chosen, a SAS 70 report provides the necessary information in five sections:

- **Section I: The Opinion**. The opinion represents the result of the audit and is based on the design of the company's controls and how they perform against certain control objectives. It is important to note that the control objectives are specified by management, not the auditor, and there is no one uniform set of control objectives.

  The opinion section of the report also states which type of report is being provided (Type I or Type II), explains which of the company services will be covered in the report, and details the systems the company uses to provide those services. In a Type I report, the auditor has a responsibility in the opinion to draw conclusions regarding the design of the controls and whether the control objectives are satisfied based on that design for the day covered by the Type I report.

  In a Type II report, the auditor has the same responsibility regarding design with an additional responsibility regarding the achievement of the control objectives based on "operating effectiveness testing over a stated period of time." It is important to note that most control objectives have multiple controls that work together to

achieve the control objective. In this case, not all controls have to be operating with a 100 percent success rate if there are suitable compensating and complementary controls that are operating effectively.

It is up to the auditors to use their judgment to determine if the control objective was achieved by considering a number of factors, including the controls tested, the results of the tests, types of testing and sample sizes, types of exceptions noted, and the presence of compensating or complementary controls and the effectiveness of those controls.

- **Section II: The Description of Controls**. The description of the control environment is written by the company's management team and highlights what controls are in place and why.
- **Section III: The Control Objectives and Controls and the Auditors Testing and Results**. This section lists the control objectives, the controls in place to achieve those objectives, the manner in which the auditor tested these controls, and the results of the testing.
- **Section IV: User Control Considerations**. This section explains any controls that the company is unable to implement or that are too costly to implement. This information is important to the company's customers to consider so that they can compensate for any gaps in the vendor's controls by implementing those controls in their own control environments.
- **Section V: Other Information Provided by Management**. This section is optional, but companies can use it to provide additional information they consider pertinent to customers and other users of the report. This section is not audited, so companies can include any information they want. As such, this section provides the company with an opportunity to put its stamp on the report and focus on those messages it most wants to communicate to its customers.

  This information can provide an overview of the organization, highlight why the company's services and controls are superior to others in the marketplace, provide relevant statistics about controls and performance, and so on. In fact, when this section is well-written, it can become another tool for use during a sales call.

Supporting a Successful Audit Process

Companies can take several steps to ensure that the audit process is successful.

1. **Appoint an internal liaison**. The SAS 70 audit itself can be initiated by anyone in the company, from the chief executive officer or chief financial officer to sales executives responding to customer demands or representatives of the company's internal audit or compliance departments.

   One person within the company, however, should be appointed liaison to the outside auditor. This liaison should work closely with the auditor to provide any necessary insight and information and to remove any organizational roadblocks that can hinder the auditor's ability to complete the work. This individual does not necessarily have to be high up in the organization, but he or she should at least report to someone who is and should be highly knowledgeable about the company and its operations.

Involving internal resources in the audit process can be valuable to an outside auditor who will not be as intimately familiar with the company's systems and processes. However, the ultimate responsibility for the audit still must be on the third-party auditor to ensure objectivity.

2. **Allow ample time for the audit and remediation process**. Companies seeking a SAS 70 report must recognize that the process generally requires more than a few weeks to complete. In some cases, the process for a Type I report can take as little as a few weeks to a few months from the initial assessment to the completion of the final report. If the company wants a Type II report, the process will require a minimum of six months to complete from the time the company hires the auditor to the completion of the final report.

   If the audit uncovers significant control weaknesses, the process can take even longer as the company works to address those problem areas. Some of the most common problems involve inadequate system security or program change control monitoring, operating systems that have not been updated with the latest security patches, and inadequate organizational policies or procedures. In some cases, companies may need to undertake non-technology-related initiatives to deal with personnel and other issues, such as providing proper and timely training where needed and helping individual employees and managers adjust to any operating changes.

   Although these issues can be a challenge in many organizations, the good news is that the overall remediation effort often focuses on strengthening existing controls rather than redesigning the entire control environment.

3. **Determine the scope of the audit**. It is important to determine exactly what will be audited. In general, the scope of the auditing process depends on the company and its control objectives, systems, and services. For example, some companies are highly automated and heavily reliant on technology in their operations, while others have few IT systems at all and handle most processes manually.

   In the former case, the audit would focus on controls surrounding IT, including specific security controls and general controls across the organization. In the less automated company, the controls would focus on those manual processes. In both cases, the project scope would specify what the audit will cover.

4. **Draft control objectives**. A key part of the audit process is drafting control objectives for the entity as a whole, IT controls, process controls, and application testing. In many cases, companies focus on the controls they think their customers and prospects will demand or controls that highlight the company's uniqueness or a specific niche.

   For example, a company that handles credit card transactions and collections for banks might have general IT-based control objectives, as well as control objectives based on the company's ability to handle collections and customer support and to maintain data and information security and confidentiality. If the company offers specific services, like direct downloading of activity reports, the control objectives could also focus on that element of operations.

5. **Be open to organizational changes as a result of the audit**. It is natural for managers and executives to be anxious about the audit process. In many cases, there is some concern that the control environment is not strong enough to meet SAS 70 requirements. Although it can be difficult to hear negative feedback, companies need to be prepared to make the necessary changes to strengthen those controls.

In many cases, strengthening controls also means changing the way things are done in the organization if control problems are traced to operational issues. Of course, making process changes to ensure adequate controls can add to a company's overhead. But more often, these changes result in increased savings and reduced risks.

For example, in one company, a SAS 70 audit revealed that the computer backup system was not working and the backup data the company had was unreadable without anyone realizing it. That same audit uncovered another situation where certain processes had three layers of review that were not necessary for adequate controls because the managers involved did not know their efforts were overlapping.

In other situations, there could be a need for more control and review of the work being done and that can sometimes cause resentment. In these cases, there may need to be a cultural shift in certain departments so that individuals build in time for necessary reviews without slowing down the workflow.

6. **Build a control mindset into the business**. Once a company goes through a SAS 70 audit, it is a good idea to frame any future process changes against the requirements of SAS 70. This not only will help ease future audits, but it can also help to build a control mindset into the company's operations.

   For example, if the company upgrades its systems, it needs to make sure that any new processes designed for the systems are aligned with the new SAS 70-based procedures and ways of doing things. Otherwise, there is a danger that individuals could revert to old habits and procedures and undermine existing controls. With a control-based mindset, companies can anticipate these issues and recognize them as soon as they occur and adjust as needed.

It is important to remember that a SAS 70 audit is not a one-time event. Most companies have a SAS 70 done annually. Some organizations may have one done every six months and others only once every two or three years.

The driving factor behind audit frequency is a company's contract with the users. If the contract requires an annual SAS 70, then the company must have an annual SAS 70 audit. Some contracts are silent on the issue of frequency so more time may pass between reports. Other companies may have a large number of public company clients with fiscal years that end at different times throughout the year, making a more frequent SAS 70 the preferred solution.

Sharing Information

The interconnectedness of business relationships has been a tremendous boon to many companies that have worked hard to solidify their relationships with both current and future customers. If that trend is to continue, companies need to continually reassure those customers that they have done everything possible to ensure that their controls meet accepted standards.

Contact Information

George Wiegand is a senior risk assessment manager based in the Indianapolis office of Crowe Chizek and Company LLC. He specializes in managing and directing SAS 70 audits and assisting the firm's financial auditors in assessing IT controls to support the financial audit. He can be reached at **317.706.2665** or **gwiegand@crowechizek.com**.

Crowe®

www.crowechizek.com

PUB7369